Подходы к построению системы безопасности в изолированных сегментах энергосистемы

Гуревич Алексей,
член ЦК «Кибербезопасность» НТИ EnergyNet,
член CIGRE

EnergyNet

Центр компетенций «КИБЕРБЕЗОПАСНОСТЬ»

cigré

Национальная технологическая инициатива Energynet (Энерджинет)

Energynet — точка сборки национальных инициатив в области создания интеллектуальной электроэнергетической систем.

Energynet

Национальная технологическая инициатива

Сформированы направления:

- ✓ активные энергетические комплексы;
- ✓ агрегаторы управления спросом;
- ✓ энергоснабжение изолированных и удаленных территорий;
- ✓ применение систем накопления и выдачи в сеть электроэнергии;
- ✓ цифровые распределительные сети;
- ✓ потребительские сервисы на базе распределённых реестров и смарт-контрактов.

Центры компетенций НТИ «Энерджинет»

Центр компетенций НТИ представляет собой структурное подразделение, создаваемое на базе вуза или научной организации, осуществляющее комплексное развитие «сквозных» технологий НТИ совместно с членами консорциума на основании договора о формировании консорциума.

Energynet

Национальная технологическая инициатива

Центры компетенций НТИ

Технологии транспортировки электроэнергии и распределенных интеллектуальных энергосистем

Автономная энергетика

Технологии новых и мобильных источников энергии

Интеллектуальная распределенная энергетика

Стандартизация и оценка соответствия

Экспертно-аналитический центр «Энерджинет»

Кибербезопасность НТИ «Энерджинет»

Архитектурный комитет

Группа НПА

Рабочая группа

Центр компетенций «Кибербезопасность» НТИ ЭнерджиНЕТ

Исследования, технологические разработки, изыскания

Тематические направления	Уникальные компетенции, научная база, научные заделы	Материально-техническая база
Кибербезопасность Информационная безопасность Информационная безопасность АСУ ТП Информационная безопасность IoT	Наличие опытных экспертов, обеспеченных необходимыми ресурсами (лаборатории, оборудование, международные и российские документы и ассоциации, технологические партнёры и т. д.) Значительное количество участников с учёной степенью	**Лаборатория и стенды кибербезопасности для ТЭК:** iGrids, РГУ (НИУ) им. И.М.Губкина, InfoWatch, Kaspersky **ПО и ПАК**: Kaspersky, InfoWatch, iGrids

Образование, обучение и подготовка кадров

Направление подготовки	Образовательный формат	Год запуска
Профессиональные тренинги по анализу кибербезопасности и расследованиям инцидентов	мастер-классы	2019
Семинары по безопасной разработке IoT приложений	мастер-классы	2019
Безопасность объектов КИИ в ТЭК	ДПО	2019

Участие в текущих проектах

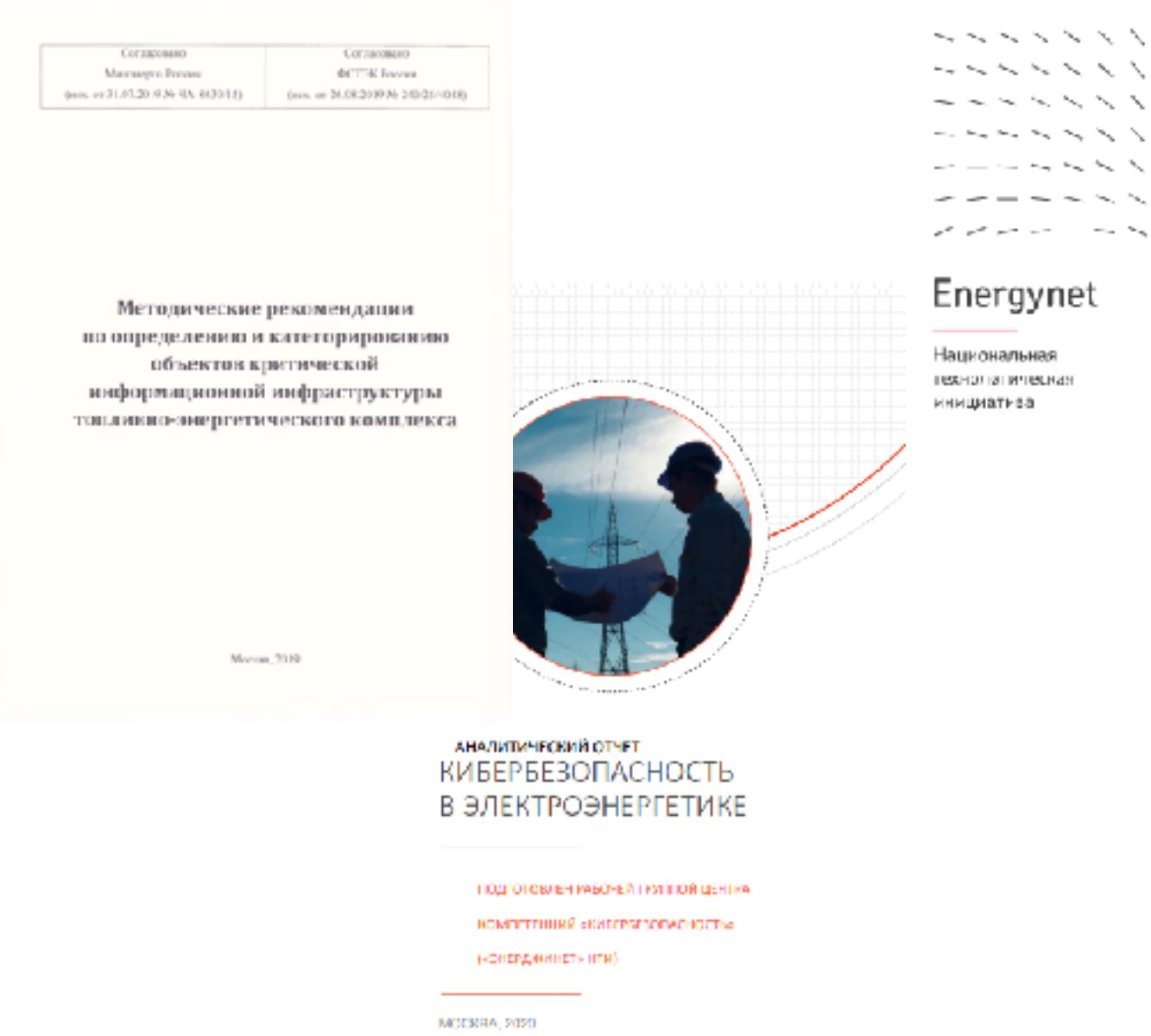
Наименование проекта (направление)	Год запуска
Разработка открытой базы знаний по Кибербезопасности	2019 по н.в.
Участие в проектах «Энерджинет»	2019 по н.в.
Участие в разработке профессиональных и образовательных стандартов по кибербезопасности	2020 по н.в.
Разработка аналитических отчетов по ИБ, участие в разработке проектов НПА, НТД	2019 по н.в.

Центр компетенций «Кибербезопасность» НТИ ЭнерджиНЕТ

В рамках работы эксперты Центра компетенций по кибербезопасности в электроэнергетике НТИ EnergyNet приняли участие в 2019 году в разработке следующих документов:

a. Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса, согласованные Министерством энергетики и ФСТЭК России (https://minenergo.gov.ru/view-pdf/11357/102517).

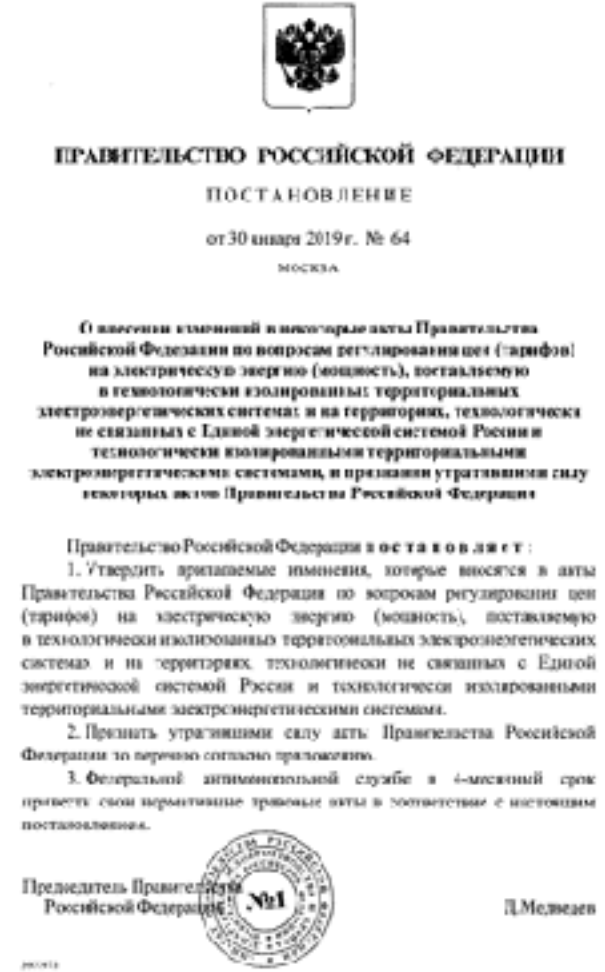
b. Аналитический отчет «Кибербезопасность в электроэнергетике», опубликованный на сайте НТИ EnergyNet в феврале 2020 (https://energynet.ru/upload/Кибербезопасность%20в%20электроэнергетике.pdf).



Регулирование работы изолированных сегментов энергосистемы (некоторые правовые акты РФ)

Постановление правительства РФ от 30 января 2019 года №64 «О некоторых вопросах регулирования тарифов на электроэнергию в технологически изолированных территориальных электроэнергетических системах».

ГОСТ Р 55105-2019 «Единая энергетическая система и изолированно работающие энергосистемы. Оперативно-диспетчерское управление. Автоматическое противоаварийное управление режимами энергосистем. Противоаварийная автоматика энергосистем. Нормы и требования» от 26 декабря 2019 (утвержден Федеральным агентством по техническому регулированию и метрологии).



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 30 января 2019 г. № 64

МОСКВА

О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам регулирования цен (тарифов) на электрическую энергию (мощность), поставляемую в технологически изолированных территориальных электроэнергетических системах и на территориях, технологически не связанных с Единой энергетической системой России и технологически изолированными территориальными электроэнергетическими системами, и признании утратившими силу некоторых актов Правительства Российской Федерации

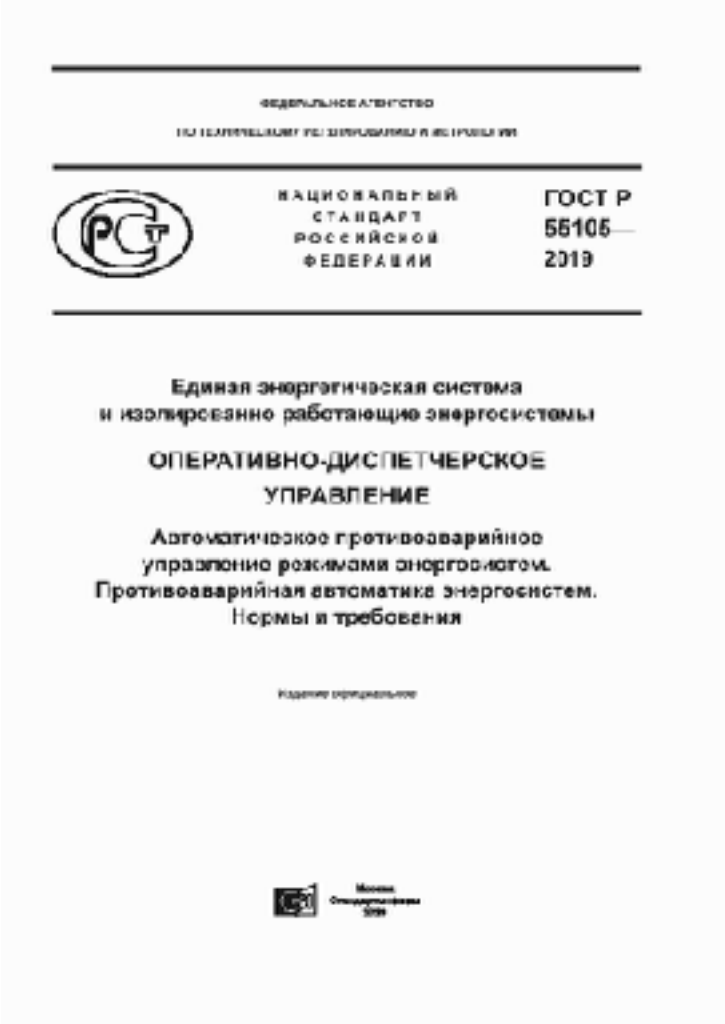
Правительство Российской Федерации п о с т а н о в л я е т :

1. Утвердить прилагаемые изменения, которые вносятся в акты Правительства Российской Федерации по вопросам регулирования цен (тарифов) на электрическую энергию (мощность), поставляемую в технологически изолированных территориальных электроэнергетических системах и на территориях, технологически не связанных с Единой энергетической системой России и технологически изолированными территориальными электроэнергетическими системами.

2. Признать утратившими силу акты Правительства Российской Федерации по перечню согласно приложению.

3. Федеральной антимонопольной службе в 4-месячный срок привести свои нормативные правовые акты в соответствие с настоящим постановлением.

Председатель Правительства Российской Федерации Д.Медведев



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 55105— 2019

Единая энергетическая система и изолированно работающие энергосистемы

ОПЕРАТИВНО-ДИСПЕТЧЕРСКОЕ УПРАВЛЕНИЕ

Автоматическое противоаварийное управление режимами энергосистем. Противоаварийная автоматика энергосистем. Нормы и требования

Подходы к построению системы безопасности в изолированных сегментах энергосистемы

Особенности рассматриваемого проекта:

1. Получение исходных данных (обследование)

- заочное обследование;
- информационное и инструментальное обследование (очное);
- подготовка отчетов об обследовании.

2. Эскизное проектирование системы защиты

3. Формирование перечня объектов КИИ подлежащих категорированию

4. Категорирование объектов КИИ

5. Формирование технического проекта

6. Внедрение системы защиты внедряемой системы энергоснабжающего комплекса

Особенности рассматриваемого проекта:

- удаленность изолированного энергорайона (расстояние до районного и областного центра: более 120 км., соседний населенный пункт — более 50 км.)
- дифференциация технологий энергоснабжающего комплекса (действующее оборудование, ветрогенерация, IoE устройства);
- полное отсутствие локального персонала для обслуживания средств защиты информации

Подходы к построению системы безопасности в изолированных сегментах энергосистемы

На этапе эскизного проектирования предложено реализовать набор мер, описанных в приказе ФСТЭК №239 для объектов 3 категории значимости

внедрение технических средств для:

- подсистемы безопасного межсетевого взаимодействия
- системы мониторинга и обнаружения вторжения
- подсистемы защиты автоматизированных рабочих мест и серверов АСУ ТП (АВП)

внедрение орг.мер, позволяющих высокий уровень безопасности удаленных объектов автоматизации:

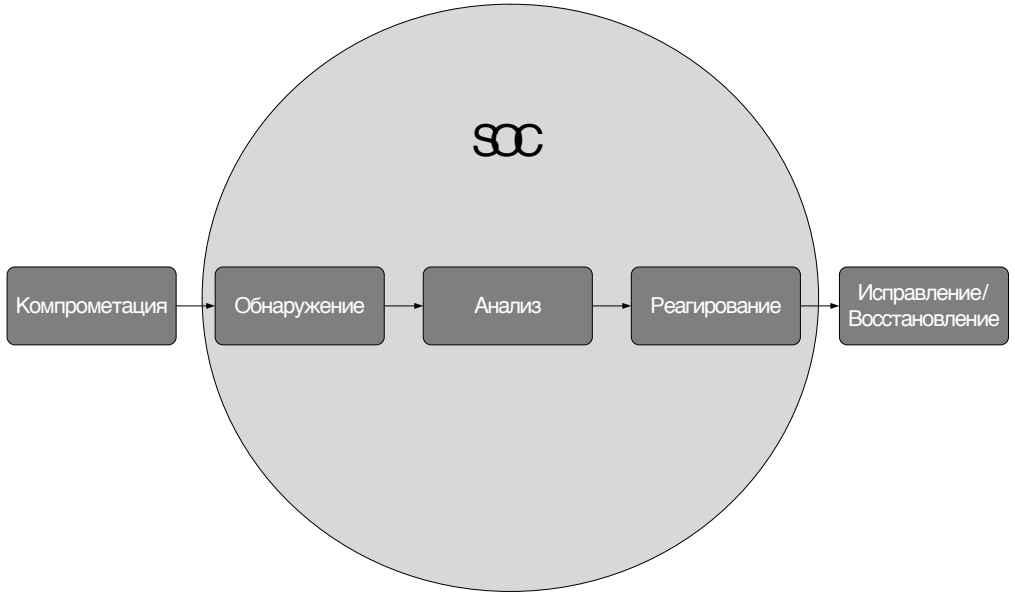
- смена всех аутентификационных данных по умолчанию на всех используемых в составе АСУ устройствах и сервисах с периодической смены аутентификационных данных (как минимум для WiFi и VPN).
- обновление прошивок, прикладного и системного ПО до актуальной стабильной версии до начала предварительных испытаний или опытной эксплуатации. Организовать процедуру тестирования и обновления ПО в случае выявления в нём уязвимостей.
- организовать процедуру периодического обновления антивирусных баз, не реже раза в месяц.
- организовать защиту каналов взаимодействия АСУ с вузом и Заказчиком
- обеспечить блокировку доступа к ресурсам сети Интернет.
- обеспечить использование политики разграничения прав сетевого доступа «Всё что явно не разрешено, запрещено». Блокировать сетевое взаимодействие с любыми неизвестными адресами.
- обеспечить (с использованием настроек ОС):
  - минимизацию прав доступа оператора;
  - блокировку использование внешних USB-устройств и носителей информации.

С учетом указанных ранее особенностей проекта одним из самых сложных и востребованных вопросов является создание системы мониторинга событий информационной безопасности в изолированном сегменте энергосистемы.

Внедрение механизмов SOC для мониторинга IoT (IoE)

Центром компетенции «Киберебзопасность» ведется работа по исследованию (разработке аналитического отчета) некоторых вопросов относительно применимости SOC для IoE, таких как:

- кто будет развивать и содержать структуру сил и средств обеспечения кибербезопасности устройств IoT (IoE)
- как будет выстроено реагирование на инциденты между предприятиями
- какие технические аспекты обеспечения информационной безопасности необходимо учитывать..



Задачами зрелого SOC являются

- Мониторинг в режиме 24x7x365.
- Высокий уровень экспертизы.
- Выстроенные процессы.
- Продвинутая аналитика, включающая Threat Intelligence и Threat Hunting.
- Выделенный аналитик, контролирующий инфраструктуру.
- Расследование/изучение каждого события безопасности.
- Индивидуальный план реагирования на инциденты.

Данный аналитический отчет позволит решить некоторые из аспектов мониторинга инфраструктуры рассматриваемого в рамках одного из аспектов построения системы обеспечения безопасности ОКИИ изолированного сегмента энергосистемы, а также войдет в состав технической брошюры, которая будет выпущена рабочей группой WG D2.51 CIGRE WG D2.51, проводящей исследование применимости SOC в том числе для IoE устройств в рамках согласованного технического задания «Implementation of Security Operations Centers (SOC) in Electric Power Industry as Part of Situational Awareness System».

Спасибо за внимание!

EnergyNet

Центр компетенций «КИБЕРБЕЗОПАСНОСТЬ»

cigré